PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

PURPOSE

Personal information is information in any form that can identify a living person.

The Privacy Act 1988 (Cth) regulates how certain private sector organisations can collect, hold, use and disclose personal information and how the individual can access and correct that information.

The purpose of this policy is to set out how we will respect and protect the personal and sensitive information of participants and their dignity and right to privacy.

This policy has been developed in accordance with the Privacy Act 1988, the Australian Privacy Principles and all applicable state or territory legislation, which outline the proper collection, use, and storage of personal information.

This policy applies to all records containing personal and/or sensitive information, whether they are in hard copy or electronic form, as well as to any interviews or discussions of a sensitive personal nature.

SCOPE

This policy applies to:

- All staff, including permanent or casual employees, contractors, consultants, and people otherwise engaged by us (e.g., volunteers).
- All participants receiving NDIS services and support, including their families and support network.

This policy covers how we collect, holds, uses and discloses the participant's personal information.

This policy applies to all personal information collected, including personal information collected through our social media channels, website and from other service providers.

DEFINITIONS

Term	Definition
Confidentiality	It means protecting the secrecy and privacy of information collected from individuals and organisations.

Data breach	A data breach happens when personal information is accessed, disclosed without authorisation or is lost. For example, when: ● a USB or mobile phone that holds an individual's personal information is stolen ● a database containing personal information is hacked ● someone's personal information is sent to the wrong person A data breach can harm an individual whose personal information is affected. They can, for example, suffer distress or financial loss. An eligible data breach occurs when the following criteria are met: ● There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur). ● This is likely to result in serious harm to any of the individuals to whom the information relates. ● The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.
Personal information	Includes a broad range of information or an opinion that could identify an individual. For example, personal information may include the following: ● an individual's name, signature, address, phone number or date of birth ● sensitive information ● credit information ● staff member record information ● photographs ● internet protocol (IP) addresses ● voiceprint and facial recognition biometrics ● location information from a mobile device.
Sensitive information	Sensitive information means: ● information or an opinion about an individual's: ○ racial or ethnic origin; or ○ political opinions; or ○ membership of a political association; or ○ religious beliefs or affiliations; or ○ philosophical beliefs; or

	○ membership of a professional or trade association; or ○ membership of a trade union; or ○ sexual orientation or practices; or ○ criminal record; or ● health information about an individual; or ● genetic information about an individual that is not otherwise health information; or ● biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or ● biometric templates.

POLICY

We are committed to providing high-quality support and services that respect the dignity and privacy of each participant.

To achieve this commitment, we will ensure that:

- Consistent processes and practices are in place that respect and protect the personal privacy and dignity of each participant.
- Each participant is advised of confidentiality policies using the language, mode of communication and terms that the participant is most likely to understand.
- Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

We respect and protects each participant's dignity and right to privacy by complying with the Privacy Act 1988, the NDIS Quality and Safeguarding Framework requirements, all applicable state or territory legislation and adhering to the Australian Privacy Principles in its information management practices.

We will maintain and protect the privacy and confidentiality of all participants and their family members, carers, guardians and/or advocates. This includes collecting, storing, and handling information about participants and the services provided to them in a way that respects their rights.

All staff and management are expected to comply with this policy, be consistent in collecting the participants' information, follow the procedures for handling their information and determine who has access to it.

Staff must ensure that each participant understands and agrees to the collection and handling of their personal information and the reasons for it. Before any audio or visual material can be recorded, the participant must give permission in writing using the *Participant Consent Form*.

Staff must also ensure that participants are aware of their rights regarding privacy and confidentiality and that they understand their obligations to protect their personal and sensitive information. To achieve this, participants will be advised of this *Privacy and Confidentiality Policy* using language, communication methods and terms that they can easily understand.

We will also ensure that the privacy and confidentiality of the personal information in relation to any staff member are protected. We follow the Workplace privacy Best Practice Guide developed by Fair Work Ombudsman to ensure we meet our obligations when managing employees' personal information. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- the employee's taxation, banking or superannuation affairs.

This policy applies to all records, including both hard copies and electronic versions, that contain personal information about individuals, as well as to any sensitive personal meetings, interviews or discussions.

PROCEDURE

The following procedures are implemented to ensure that we meet our policy objective of ensuring that the privacy and confidentiality of each participant are protected when accessing our supports and services.

COLLECTION OF PERSONAL INFORMATION

During the intake and initial assessment processes and throughout service delivery, participants are informed of the types of information that will be collected about them, how their privacy will be safeguarded, and their rights in relation to their personal and sensitive information. The *Participant Handbook* and *Service Agreement* that are included in the Participants' Welcome Pack also provide information about their rights to privacy and confidentiality.

We may collect personal information about a participant from them, their representative or a third party such as a service provider that is referring the participant to us. Our organisation or people acting on its behalf (e.g., contractors) may also collect information directly.

We will not ask participants for any personal information that we do not need. The Privacy Act requires that we collect information for a purpose that is reasonably necessary for or directly related to its services or operations.

When staff collects personal information, they are required by the Privacy Act to notify participants of several matters. These include the purposes for which we collect the information, whether the collection is required or authorised by law and any person or body to whom we usually disclose the information. We generally provide this notification by having Privacy Notices on our paper-based forms and online portals.

We collect personal information through a variety of different methods including, but not limited to:

- paper-based forms
- electronic forms (including online forms)
- face-to-face meetings
- telephone communications
- email communications
- communications by fax
- Our website; and
- Our social media channels.

All personal and sensitive information must be collected, used, retained, and disclosed with the participant's consent only. Where required, Staff must collect the participant's consent using the *Participant Consent Form* or any other forms approved by us, which will be stored on the participant's file.

The type of personal information collected, the purpose for keeping it, the methods used for collection, use, or disclosure, and who will have access to it are clearly communicated to participants.

We hold personal information in a range of paper-based and electronic records. In delivering its services and performing its duties, we collect and holds the following kinds of personal information (which will vary depending on the context of the collection):

- name, address and contact details (e.g., phone, email);
- photographs, video recordings and audio recordings of the participant;
- information about the participant's personal circumstances (e.g., marital status, age, gender, occupation, accommodation and relevant information about their partner or children);
- information about their identity (e.g., date of birth, country of birth);
- information about their background (e.g., the languages they speak, cultural background); and
- government identifiers (e.g., NDIS Number, Centrelink Reference Number).

We may also collect or hold some sensitive information about the participant, including information about their:

- racial or ethnic origin;
- health (including information about their medical history and any disability or injury they may have);
- Information about the supports or services they receive from other service providers; and
- information about the people who provide those supports or services to them.

When collecting the participants' personal information, staff must:

- Collect and store personal information from participants that is necessary for the provision of our supports and services and that is given voluntarily only.
- Utilise fair and lawful methods for collecting personal information.
- Obtain consent from participants and their carers before collecting personal information.
- Assure participants and their families and support network that their right to privacy and confidentiality is being upheld when conducting any meeting, interview or discussion of personal or sensitive nature.
- Communicate to participants and their family/carers/guardians about the type of personal information being collected and the reason for its collection, the methods used for collecting, using or disclosing it, and who will have access to it.
- Ensure participants agree in writing to any recordings made in an audio or visual format using the *Participant Consent Form*.

PURPOSES FOR WHICH PERSONAL INFORMATION IS COLLECTED, HELD, USED AND DISCLOSED

We collect and holds personal and sensitive information of participants for a variety of different purposes relating to its responsibilities under the Service Agreement and operations, including, but not limited to:

- Intake and referral processes.
- Support planning and reviews.
- Delivering its services and supports to participants.
- Internal and external audits.
- Complaints handling.
- Incident management and investigation.
- Management of correspondence.

We use and disclose personal information for the primary purposes for which it is collected. Staff must give participants and/or their families, carers, guardians or advocates information about the primary purpose of collection at the time the information is collected we will only use your personal information for secondary purposes where it is able to do so in accordance with the Privacy Act, for example, where disclosure is required or authorised by the National Disability Insurance Scheme Act 2013

We may disclose the participant's personal information collected and held by it to other relevant parties, including the NDIA, state or territory agencies or authorities, regulatory bodies or other service providers, where we have the participant's consent or where we are otherwise legally able or required to do so.

HANDLING PERSONAL INFORMATION

All staff members are responsible for handling personal information they have access to with care, ensuring that privacy and confidentiality are protected and always upheld.

When handling personal information, staff must:

- Ensure that collected personal information is accurate, complete, and up to date, allowing individuals to review or correct any information about themselves.
- Take reasonable measures to protect personal information from misuse, loss, unauthorised access, modification, or disclosure. This includes:
    - Ensuring privacy during interviews or discussions of a sensitive nature.
    - Collecting personal information only with consent from the individual.
    - Keeping all hard copy files of participant records securely in a locked filing cabinet safeguarded by the Director.

    - Ensuring all electronic files are password protected to ensure confidentiality and security.
- Destroy or permanently de-identify personal information that is no longer needed or that has reached the end of legal retention requirements, with the authorisation of the Privacy Officer.
- Maintain the privacy of participants' information throughout the provision of supports and services.
- Store all personal information and written consent from the participants and/or their families/carers in the participant's file.
- Verify that information provided by other agencies or external individuals aligns with our privacy principles.
- Inform participants that they have the option to opt out of any NDIS information sharing during audits.
- Obtain participants' consent before referring them to another service provider, as the referral process involves sharing personal information.
- Obtain consent from participants for any information sharing between us and any government agencies.

Supervisors and/or line managers are responsible for ensuring that:

- Appropriate consent is obtained for the inclusion of any personal information about any individual, including our personnel.
- All staff members understand and follow this policy and procedure for handling personal information.

The Privacy Officer or their delegate is responsible for the following:

- Including a Privacy Statement on our website that clearly explains the conditions for the collection of personal information from the public visiting the website.
- Protecting personal information related to our staff, management, and contractors.
- Acting as Privacy Officer and addressing any queries or complaints regarding privacy issues.

The confidentiality of participant records will be maintained by staff members who are directly involved in providing services to the participant. The information contained in these records will only be shared with other parties if the participant, their advocate, guardian, or legal representative gives their consent.

Staff are required to take all reasonable steps to protect and maintain the privacy and confidentiality of personal and sensitive information for all participants, their families and support network, staff, and management.

The Senior Management Team must ensure that any additional security measure is appropriately implemented to protect personal and sensitive information from participants and staff.

Participants are encouraged to raise complaints if they think that their right to privacy and confidentiality is not being protected by us. The *Feedback and Complaints Management Policy and Procedure* will be followed to manage all complaints raised by the participants effectively.

ACCESS AND CORRECTION OF PERSONAL INFORMATION

Participants and staff have a right under the Privacy Act to access personal information held about them. Participants and staff also have a right under the Privacy Act to request corrections to any personal information that we hold about them if they think the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading. However, the Privacy Act sets out circumstances in which we may decline access to or correction of personal information (e.g., denying access is required or authorised by or under an Australian law or a court/tribunal order).

To access or seek correction of personal information we hold about them, participants must contact us by phoning our office or mobile.

DATA SECURITY

Access to personal information held is restricted to authorised persons who are staff or contractors. Electronic and paper records containing personal information are protected as per the *Information Management Policy and Procedure*.

We regularly conduct internal audits to ensure our organisation adheres to our protective and computer security policies.

DATA BREACH MANAGEMENT

We will take this matter seriously and deal promptly with any accidental or unauthorised disclosure of personal information. We follow the OAIC's data breach notification guide when handling accidental or unauthorised disclosures of personal information.

We recognise the seriousness of data breaches and has put in place robust systems and procedures to detect and respond effectively.

Under the Notifiable Data Breaches scheme, we are obligated to inform any individual and the Office of the Australian Information Commissioner (OAIC) if a data breach is likely to cause them serious harm. The NDB scheme is designed so that only serious ('eligible') data breaches are notified.

Staff are trained and instructed to inform their supervisor or line manager or the Privacy Officer immediately if they suspect or become aware of a potential data breach. If unsure how to manage a data breach, staff must seek advice from their supervisor or line manager directly.

The Director has appointed the Privacy Officer role, as well as certain staff members who have the necessary knowledge and skills to be part of the Data Breach Response Team. The members of the Data Breach Response Team, along with their key functions, are listed in the *Human Resource Register*.

The Data Breach Response Team is responsible for the following:

- Collecting and documenting all information and available evidence required to assess the suspected breach.
- Consult with relevant staff members regarding specific circumstances.
- Notify all individuals whose personal information is involved in the data breach that are at risk of serious harm.
- Develop and follow the *Data Breach Response Plan* to respond to all potential risks associated with data breaches.
- Follow the instructions given by the Privacy Officer to implement immediate remedial actions to reduce any potential harm to individuals caused by a suspected or eligible data breach.
- Engage independent cybersecurity or a forensic expert, as appropriate.
- Make recommendations to the Privacy Officer whether the data breach constitutes an eligible data breach or not and any remedial actions to be taken.
- Develop a communication or media strategy to reduce the impact on our reputation due to the data breach or suspected data breach. This includes determining the method of communication and content.

The Privacy Officer is responsible for notifying the Office of the Australian Information Commissioner (OAIC) of any data breach that is likely to result in serious harm to an individual whose personal information is involved.

The Data Breach Response Team has developed the *Data Breach Response Plan*, which incorporates any remedial action or steps to reduce any potential harm to individuals caused by a suspected or eligible data breach and manage any reputational risks to our

business. It incorporates the requirements of the NDB scheme for assessing and responding to suspected eligible data breaches.

The data breach management procedure includes the following stages:

1) **Assessment and identification of eligible data breaches**

If we suspect that it may have experienced an eligible data breach, it must quickly assess the situation to decide whether there has been an eligible data breach. We have 30 days to assess whether a data breach is likely to result in serious harm.

The Privacy Officer will assess any data breach or suspected data breach and determine if the data breach is likely to result in serious harm to an individual. An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters:

- the kind and sensitivity of the information subject to the breach
- whether the information is protected and the likelihood of overcoming that protection
- if a security technology or methodology is used in relation to the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to circumvent the security technology or methodology
- the persons, or the kinds of persons, who have obtained, or could obtain, the information.
- the nature of the harm that may result from the data breach.

The assessment must be reasonable and expeditious, and the Privacy Officer must follow the following procedures for assessing a suspected data breach:

- **Initiate:** Decide whether an assessment is necessary.
- **Investigate:** Quickly gather relevant information about the suspected breach, including, for example, what personal information is affected, who may have had access to the information, and what the likely impacts are.
- **Evaluate:** Make a decision, based on the investigation, about whether the identified breach is an eligible data breach or not.
- **Immediate remedial actions:** During the course of an assessment, or when the assessment is complete, determine which remedial actions must be taken immediately to reduce any potential harm to individuals caused by a suspected or eligible data breach.
- **Record Keeping:** Document the assessment process and outcome using the *Data Breach Assessment Report*.

2) Remedial actions

The Notifiable Data Breaches scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner and avoid the need to notify.

At any time, including during an assessment, the Data Breach Response Team can and should take any remedial action or steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. Remedial action may include retrieval or recovery of the personal information, shutting down or isolating the affected system, ceasing unauthorised access etc.

If remedial action is successful in preventing serious harm to affected individuals, notification to individuals and the Office of the Australian Information Commissioner (OAIC) is not required.

A team member of the Data Breach Response Team will complete the *Data Breach Process Report* within 48 hours of receiving instructions from the Privacy Officer to implement immediate remedial actions. The report will contain the following:

- The description of the data breach or suspected data breach.
- Summary of action taken.
- Summary of outcomes from the action taken.
- Processes implemented to prevent a repeat situation.
- Explanation outlining why no further action is necessary.
- Signature of the Privacy Officer confirming that no further action is required.

3) Notification to individuals and the OAIC

Once we is aware that there are reasonable grounds to believe that there has been an eligible data breach — whether during the course of an assessment or when the assessment is complete — the Data Breach Response Team members must promptly notify affected individuals and the Office of the Australian Information Commissioner (OAIC) about the breach.

The Data Breach Response Team must notify individuals of the data breach immediately if they have reasonable grounds to believe that they are at risk of being affected by the data breach. The notification to individuals and OAIC will be made in the form of a statement, and it must include the following:

- The identification and contact details of our organisation and any other entity that jointly or simultaneously holds the same information. If information of this sort is included in the notification, the other entity will not need to report the eligible data breach separately.

- The description of the data breach.
- the kinds of information involved; and
- recommendations about the steps they should take in response to the data breach. This may include recommendations about changing passwords, contacting the police if their physical safety is at risk, contacting their doctor if they are experiencing distress, etc.

Individuals or organisations will be notified by email, telephone or post, depending on the circumstances. If direct notification is not practicable, we will publish the statement on its website and take reasonable steps to publicise its contents using different channels.

The Privacy Officer must notify the Office of the Australian Information Commissioner (OAIC) using the online *Notifiable Data Breach Form*. The notification of a data breach to the OAIC must occur within 30 days of becoming aware of the breach or suspected breach.

If participants think that a data breach may affect their personal information and they have not been notified, they should contact the Privacy Officer and ask them for information about the data breach (including whether their personal information was affected).

Participants can also complain to the Office of the Australian Information Commissioner (OAIC) if they think we did not notify them quickly enough about a data breach that involved their personal information or if they think a data breach raises other privacy issues.

Participants must first complain to us and give us a reasonable period to respond (30 days is a reasonable period). If we do not respond to their complaint, or they are not satisfied with our response, participants can complain to the Office of the Australian Information Commissioner (OAIC) by submitting the following form: https://www.oaic.gov.au/privacy/privacy-complaints.

4) Continuous Improvement Plan

Once the data breach has been dealt with appropriately, the Data Breach Response Team should focus on the following tasks:

- Examining what was learned and implementing measures to prevent similar breaches in the future, such as reviewing policies and procedures and providing additional training.
- Compiling a report for submission to the Senior Management Team.
- Considering the possibility of conducting further investigations or assessments.
- Updating the Continuous Improvement Plan and Register accordingly.

RELATED DOCUMENTS

- Participant Handbook
- Participant Consent Form
- Service Agreement
- Data Breach Response Plan
- Data Breach Assessment Report
- Staff Training Plan
- Staff Handbook
- Continuous Improvement Plan
- Continuous Improvement Register
- Easy-to-read documents
- Complaint Report Form
- Feedback and Complaints Register
- OAIC's Notifiable Data Breach form

REFERENCES

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APP)
- National Disability Insurance Scheme Act 2013 (Cth)
- National Disability Insurance Scheme (Complaints Management and Resolution) Rules 2018
- National Disability Insurance Scheme (Incident Management and Reportable Incidents) Rules 2018
- NDIS Practice Standards and Quality Indicators – November 2021
- Fair Work Ombudsman. Workplace Privacy - Best Practice Guide. January 2023
- Freedom of Information Act 1982 (Cth)
- OAIC's website - Notifiable data breaches
- Privacy and Personal Information Protection Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Privacy and Data Protection Act 2014 (VIC)
- Health Records Act 2001 (VIC)"
- Information Privacy Act 2009 (QLD)
- NOT APPLICABLE. South Australia do not have specific privacy legislation. Refer to the Privacy Act 1988 (Cth)
- NOT APPLICABLE. Western Australia do not have specific privacy legislation. Refer to the Privacy Act 1988 (Cth)
- Personal Information and Protection Act 2004 (TAS)
- Information Privacy Act 2014 (ACT)
- Information Act 2002 (NT)

REVIEW DETAILS

Approval Authority:	Operation manager
Approval Date:	2026-02-06
Last Update Date:	2026-02-06
Next Review Date:	2027-03-05
Version Control No.:	v.1.0